PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-067399
(43)Date of publication of application : 16.03.2001

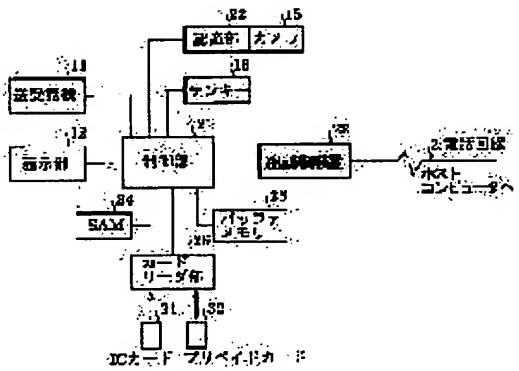
(51)Int.Cl. G06F 17/60
G06F 19/00
G06T 7/00
G07D 9/00
H04M 3/42
H04M 11/00
H04M 15/00

(21)Application number : 11-237667
(22)Date of filing : 25.08.1999

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : TAKIZAWA TOSHIO

(54) ELECTRONIC MONEY TRANSACTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To load the electronic money by means of a general telephone circuit.
SOLUTION: In this electronic money transaction system, the irises of an operator of a public telephone set are photographed by a camera 15 and recognized at a recognition part 22. Meanwhile, the personal information stored in an IC card 31 is read at a card reader part 26. The card 31 stores the registered two iris data and a control part 21 compares these iris data with each other to authenticate the identity of the operator. When this identity is authenticated, the loaded amount of electronic money is inputted to generate the communication data including the loaded amount. The communication data are enciphered and then transmitted to a host computer via a telephone circuit 2.



LEGAL STATUS

[Date of request for examination] 20.02.2006
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Between the terminal which the dealings candidate of a financial institution operates, and the host computer of a financial institution In the cybermoney trading system which conducts dealings by cybermoney through a communication line, while using the telephone line for said communication line While registering a dealings candidate's biometrics information into the IC card which informational R/W was possible and contained the central processing unit and the storage means, said terminal When an IC card is judged by IC card authentication means to judge the truth of an IC card, and this IC card authentication means to be truth, An information reading means to read the information stored in the IC card, and a biometrics information acquisition means to acquire the biometrics information of an operator to the operator concerned who operated the terminal and performed the dealings demand, The biometrics information acquired by said biometrics information acquisition means is compared with the biometrics information of the information read by the information reading means. the dealings candidate by whom the operator of a terminal was registered into the IC card -- him who attests whether you are him -- an authentication means -- this -- with a he authentication means a dealings candidate -- with a dealings demand information input means to receive dealings by cybermoney and to input dealings demand information, when it is attested that he is him A terminal side transmitting means to perform security processing, to generate commo data to information including the dealings demand information that it was inputted by this dealings demand information input means, and to transmit this commo data to a host computer through the telephone line, When reply data are answered from a host computer corresponding to the transmitted commo data, It has the terminal side receiving means which takes out the dealings processing information which shows the processing result of dealings from these reply data. Said host computer The host side receiving means which receives the commo data from a terminal and takes out dealings demand information from this commo data, A dealings processing means to perform processing about dealings based on the dealings demand information taken out by this host side receiving means, A host side transmitting means to perform security processing, to generate reply data to information including the dealings processing result processed and outputted by this dealings processing means, and to transmit these reply data to the transmitting agency terminal of commo data through the telephone line, The cybermoney trading system characterized by preparation ******.
[Claim 2] Said biometrics information is a cybermoney trading system according to claim 1 characterized by being the information on the iris image of the eyes of a dealings candidate and an operator.
[Claim 3] It is the cybermoney trading system according to claim 1 or 2 characterized by being constituted so that may record the telephone number of a connection place host computer on said IC card, the information reading means of said terminal may read the telephone number concerned in an IC card, a terminal side transmitting means may be connected to a connection place host computer based on the read telephone number and commo data may be transmitted.
[Claim 4] While the cryptographic key for a communication link and the decode key for a communication link corresponding to said IC card and host computer are stored, respectively, the information reading means of said terminal The cryptographic key for a communication link is read in an IC card. A terminal side transmitting means As security processing, information is enciphered using the cryptographic key for a communication link read in the IC card. Said terminal side receiving means It is constituted so that the reply data transmitted from the host computer using the decode key read in the IC card may be decrypted. The host side receiving means of said host computer The commo data transmitted from the terminal as security processing using the stored decode key for a communication link is decrypted. Said host side transmitting means The cybermoney trading system of any one publication of claim 1 characterized by being constituted

so that information may be enciphered using the stored cryptographic key for a communication link - claim 3.
[Claim 5] It is the cybermoney trading system according to claim 4 characterized by being constituted so that the cryptographic key for a communication link and the decode key for a communication link which were stored in the IC card using the card ID which the card ID of an IC card proper was stored in said IC card, and the information reading means of said terminal read the card ID concerned, and read may be read.
[Claim 6] Said card ID is a cybermoney trading system according to claim 5 characterized by being enciphered.
[Claim 7] While said host computer stores the card ID decode key which decrypts the enciphered card ID, the terminal side transmitting means of said terminal It is constituted so that the enciphered card ID may be included in commo data and it may transmit to a host computer. Said host side receiving means Take out the card ID enciphered from commo data, and Card ID is decrypted using the card ID decode key stored in the host computer. It is constituted so that the decode key for a communication link stored in the host computer using the decrypted this card ID may be taken out. Said host side transmitting means The cybermoney trading system according to claim 6 characterized by being constituted so that the cryptographic key for a communication link stored in the host computer using the card ID decrypted by the host side receiving means may be taken out.
[Claim 8] Said terminal is the cybermoney trading system of any one publication of claim 1 characterized by being a coin box set - claim 7.
[Claim 9] Said terminal is the cybermoney trading system of any one publication of claim 1 characterized by being a personal computer - claim 7.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention attests off-line using an IC card and biometrics information, and relates to the cybermoney trading system which trades in cybermoney through the telephone line.
[0002]
[Description of the Prior Art] in order to prevent injustice in the conventional cybermoney trading system -- a personal identification number -- using -- him, a dealings candidate, -- it is made to attest.
[0003] However, in the system using this personal identification number, in order to raise security nature, it will become expensive on a system including hardware and software. then, biometrics information peculiar to recent years and him -- using -- him -- the system which attests is developed.
[0004]
[Problem(s) to be Solved by the Invention] however, such biometrics information -- using -- him -- also in the conventional cybermoney trading system which attests, in order to raise security nature, it was difficult to perform loading of cybermoney using the circuit of dedication, and not to go to the reason for saying that this loading is performed easily always anywhere, but to also reduce communication link cost. Therefore, if loading of cybermoney can be performed using the general telephone line, dealings by cybermoney can be conducted easily.
[0005]
[Means for Solving the Problem] This invention adopts the next configuration in order to solve the above point.
<Configuration 1> the cybermoney trading system concerning invention of claim 1 Between the terminal which the dealings candidate of a financial institution operates, and the host computer of a financial institution In the cybermoney trading system which conducts dealings by cybermoney through a communication line, while using the telephone line for said communication line An IC card authentication means by which said terminal judges the truth of an IC card while registering a dealings candidate's biometrics information into the IC card which informational R/W was possible and contained the central processing unit and the storage means, An information reading means to read the information stored in the IC card when an IC card is judged by this IC card authentication means to be truth, A biometrics information acquisition means to acquire the biometrics information of an operator to the operator concerned who operated the terminal and performed the dealings demand, The biometrics information acquired by said biometrics information acquisition means is compared with the biometrics information of the information read by the information reading means. the dealings candidate by whom the operator of a terminal was registered into the IC card -- him who attests whether you are him -- an authentication means -- this -- with a he authentication means a dealings candidate -- with a dealings demand information input means to receive dealings by cybermoney and to input dealings demand information, when it is attested that he is him A terminal side transmitting means to perform security processing, to generate commo data to information including the dealings demand information that it was inputted by this dealings demand information input means, and to transmit this commo data to a host computer through the telephone line, When reply data are answered from a host computer corresponding to the transmitted commo data, The terminal side receiving means which takes out the dealings processing information which shows the processing result of dealings from these reply data, A host side receiving means by which a preparation and said host computer receive the commo data from a terminal, and take out dealings demand information from this commo data, A dealings processing means to perform processing about dealings based on the dealings demand information taken out by this host side receiving means, To information including the dealings

processing result processed and outputted by this dealings processing means, security processing is performed, reply data are generated, and it has a host side transmitting means to transmit these reply data to the transmitting agency terminal of commo data through the telephone line.
[0006] <Configuration 2> In the cybermoney trading system concerning invention of claim 2, said biometrics information is the information on the iris image of the eyes of a dealings candidate and an operator.
[0007] <Configuration 3> The telephone number of a connection place host computer is recorded on said IC card, the information reading means of said terminal reads the telephone number concerned in an IC card, and a terminal side transmitting means connects with a connection place host computer based on the read telephone number, and it consists of cybermoney trading systems concerning invention of claim 3 so that commo data may be transmitted.
[0008] <Configuration 4> in the cybermoney trading system concerning invention of claim 4 While the cryptographic key for a communication link and the decode key for a communication link corresponding to said IC card and host computer are stored, respectively The information reading means of said terminal reads the cryptographic key for a communication link in an IC card. A terminal side transmitting means as security processing Information is enciphered using the cryptographic key for a communication link read in the IC card. It is constituted so that said terminal side receiving means may decrypt the reply data transmitted from the host computer using the decode key read in the IC card. The host side receiving means of said host computer as security processing The commo data transmitted from the terminal using the stored decode key for a communication link is decrypted, and it is constituted so that said host side transmitting means may encipher information using the stored cryptographic key for a communication link.
[0009] <Configuration 5> The card ID of an IC card proper is stored in said IC card, and the information reading means of said terminal consists of cybermoney trading systems concerning invention of claim 5 so that the cryptographic key for a communication link and the decode key for a communication link which were stored in the IC card using the card ID which read and read the card ID concerned may be read.
[0010] <Configuration 6> Said card ID is enciphered in the cybermoney trading system concerning invention of claim 6.
[0011] <Configuration 7> in the cybermoney trading system concerning invention of claim 7 While the card ID decode key with which said host computer decrypts the enciphered card ID is stored It is constituted so that the terminal side transmitting means of said terminal may include the enciphered card ID in commo data and it may transmit to a host computer. Said host side receiving means takes out the card ID enciphered from commo data. Card ID is decrypted using the card ID decode key stored in the host computer. It is constituted so that the decode key for a communication link stored in the host computer using the decrypted this card ID may be taken out. Said host side transmitting means is constituted so that the cryptographic key for a communication link stored in the host computer using the card ID decrypted by the host side receiving means may be taken out.
[0012] <Configuration 8> In the cybermoney trading system concerning invention of claim 8, said terminal is a coin box set.
[0013] <Configuration 9> In the cybermoney trading system concerning invention of claim 9, said terminal is a personal computer.
[0014]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using an example.
<Example 1> An example 1 is made to perform loading of cybermoney from the coin box set as a terminal using an IC card, using the telephone line as a communication line.
[0015] Drawing 1 is the block diagram showing the configuration of an example 1, and drawing 2 is the perspective view showing the appearance of the coin box set 1 which contained the configuration of drawing 1 . As shown in drawing 2 , the side face of a coin box set 1 is equipped with a headset 11, and a display 12, a ten key 13, the IC card insertion opening 14, and the receipt exhaust port 16 are arranged in the front panel.
[0016] A ten key 13 is a dealings demand information input means to use it for having 12 keys and inputting a partner's telephone number and the load amount of money of cybermoney. A display 12 is a display which used liquid crystal, and can also display an image besides an alphabetic character.
[0017] The camera 15 as a biometrics information acquisition means is arranged in the upper part of this display 12. This camera 15 is for having CCD (charge coupled device: charge-coupled device), photoing an operator's eyes, and obtaining the image of the iris (iris) as biometrics information.

[0018] The iris is a thin film which is between the cornea of an eyeball, and a lens and has a pupil in the center. The amount of the light which controls closing motion of a pupil and enters in an eyeball is adjusted, youth is completed, and this iris has a pattern which is different with every everybody. Although this pattern is different also by the right eye and the left eye, it hardly changes through a life span. Therefore, the information on the iris turns into leading biometrics information which only he can just hold.
[0019] In addition, as biometrics information, it is not restricted to the iris and the information on a sign, a retina, a voiceprint, facies, a fingerprint, and a note can also be used. When using the information on a sign, a voiceprint, facies, a fingerprint, and a note, a biometrics information acquisition means by which such information can be acquired is used instead of a camera 15. however -- if this iris pattern is used -- a sign, a fingerprint, a voiceprint, etc. -- comparing -- the small amount of data -- him -- since it can attest, it is advantageous. This is an option although the receipt exhaust port 16 is an outlet which discharges a receipt.
[0020] Drawing 3 It is the system configuration Fig. of an example 1. A network 3 is a network where the host computer of a bank 5 was connected, and a network 4 is a network where a card issuer's 6 computer was connected. The coin box set 1 is further connected to the host computer of a bank 5 through the network 4 at a card issuer's 6 host computer through the telephone line 2 and a network 3. And at the time of banking card settlement of accounts, loading of cybermoney is performed between a coin box set 1 and the host computer of a bank 5, and when it is a credit card transaction, loading of cybermoney is performed between a coin box set 1 and a card issuer's 6 host computer.
[0021] This coin box set 1 contains a control section 21, a communication controller 23, the recognition section 22, SAM (Security Application Module)24, buffer memory 25, and the card reader section 26, as shown in drawing 1 .
[0022] A control section 21 is equipped with an interface with a microcomputer, Circumferences ROM and RAM, and I/O etc., and is constituted, and the headset 11, the display 12, and the ten key 13 grade are also connected to this control section 21. And a control section 21 performs loading of cybermoney according to the flow chart which controls a coin box set 1 and is mentioned later.
[0023] The recognition section 22 is to connect with a camera 15, to create the digital data of the image of the iris (iris) of an eye based on the image of the eyes of the operator arrested with the camera 15, once accumulate this digital data, and for this data and another data perform authentication processing of whether to be him.
[0024] SAM24 is an IC card authentication means to use it in order to attest the truth of IC card 31, and has the almost same configuration as IC card 31. The buffer memory 25 for a communication link is for once storing the information transmitted and received.
[0025] CCE 23 is equipped with a modem/NCU, is equipment which performs communications control and is connected to the host computer of a bank 5 or a card issuer 6 via the telephone line 2 and an ISDN circuit.

[0026] The card reader section 26 is an information reading means which receives IC card 31, for example, a prepaid card like a telephone card, and carries out read/write of the data. In addition, a prepaid card is an option.
[0027] the card constituted by IC card 31 embedding IC (integrated circuit) chip at that card base material -- it is -- this IC card 31 -- a dealings candidate -- his individual humanity news is recorded. RAM (Random Access Memory) for memorizing temporarily CPU (central processing unit), ROM (Read Only Memory) in which various processing programs were written, the contents of dealings, etc., and EEPROM (Electrically Erasable andProgrammable ROM) which is the nonvolatile memory in which elimination of storage information and writing are possible electrically are prepared in IC chip of this IC card 31. The control circuit which furthermore controls reading of the store circuit for making data memorize and the information on each of such memory and writing for this IC chip is also formed in one. The terminal area connected to IC chip is exposed to the front face of this IC card 31, and informational R/W is performed through this terminal area. In addition, the IC card without the contact section is also developed and such a noncontact IC card can be similarly used as opened to ISO10536 or ISO14443 in recent years.
[0028] Drawing 4 is the explanatory view showing the file organization of IC card 31 of an example 1. The file stored in IC card 31 is hierarchized, two or more exclusive files are under a master file, and there is an elementary file in the bottom of it further. Individual humanity news, such as Card ID, a personal name, iris data, the cryptographic key for personal identification numbers, the load amount of money, the connection telephone number, the account number, a load amount-of-money decode key, and a card ID decode key, is recorded on this elementary file 1, and the cryptographic key for a communication link and the decode key for a communication link are recorded on the elementary file 2.

[0029] In addition, Card ID is information used when reading the information on the cryptographic key for a communication link, and the decode key for a communication link, and it is enciphered in order to raise security nature. Moreover, iris data are data about the above-mentioned iris pattern, and the data size is 256 bytes.
[0030] This IC card 31 is deactivated and has come to be unable to perform R/W of data until a connection terminal is connected to the terminal (not shown) of the IC card insertion opening 14, in order to avoid breakage of IC card 31. In order to write data to this IC card 31, it is necessary to activate IC card 31 according to the procedure specified to JIS JISX6306.
[0031] Drawing 5 is the block diagram showing the configuration of the host computer of a bank 5 or a card issuer 6. The host computer 41 is equipped with files 42-44. A file 42 is a file for logs, a file 43 is a file which stored the decode key of Card ID, and a file 44 is a file which stored the cryptographic key for a communication link, the decode key for a communication link, and the decode key for personal identification numbers.
[0032] <Actuation of an example 1> Drawing 6 and drawing 7 are flow charts which show actuation of an example 1. At step (it is described as "S" among drawing.) 1, since it is filled up with cybermoney to its own IC card 31, an operator inserts IC card 31 in the IC card insertion opening 14, and he absorbs this IC card 31.
[0033] At step 2, mutual recognition is performed using SAM24 and the truth of IC card 31 is judged. The EXTERNAL AUTHENTICATE command specified to JIS JISX6306 of an IC card or an INTERNALAUTHENTICATE command is used for mutual recognition, and it is performed using a code technique. An EXTERNAL AUTHENTICATE command is a command used when enciphering in the IC card 31 exterior and making an authentication result calculate within IC card 31, and is INTERNAL. The AUTHENTICATE command is a command used when giving the information which serves as a seed from the exterior, for example, a random number, enciphering and judging the authentication result externally. A message is displayed on the display 12 of a coin box set 1 among mutual recognition.
[0034] Drawing 8 is the explanatory view showing the example of a display of the message displayed on a display 12. As shown in this drawing 8 (A), the message "wait for a while" "during card authentication" is displayed on a display 12 among mutual recognition. And when a card is attested with truth, it progresses to step 3. At step 3, an operator's eyes are photoed using a camera 15 and an operator's iris image is captured.
[0035] At this time, as shown in drawing 8 (B), the message "I do your check" and "look at the lens of the point of an arrow head" is displayed, and an operator's attention is attracted. And in order to centralize an eye line on a display 12 as much as possible, flashing etc. carries out an arrow head. The recognition section 22 changes the captured iris image into digital data, and obtains 256 bytes of iris data.
[0036] The iris data registered are read in IC card 31 at step 4. Reading is performed by the card reader section 26. This iris data is stored in the elementary file as shown in drawing 4 .
[0037] At step 5, the iris data incorporated from the camera 15 are compared with the iris data read in IC card 31, and his recognition is performed. The technique indicated by for example, the U.S. Pat. No. 5,291,560 official report is used for this iris authentication. When he is able to be attested, it progresses to step 8.
[0038] Moreover, when he is not able to be attested, it progresses to step 6, and it judges whether it is the predetermined less than count of a retry, for example, 3 times. When the count of a retry is 3 or less times, it returns to step 3 and his authentication is performed again. At this time, the message of a purport which gives an operator his authentication once again is displayed on a display 12.
[0039] When the count of a retry is able to attest him by 3 or less times, it progresses to step 8. moreover, the time of the count of a retry exceeding 3 times -- an operator -- a dealings candidate -- it judges with his not being him, and progresses to step 7, and halt processing of dealings is performed. An operator is made to input a personal identification number and you may make it check at this time. When a personal identification number is inputted, it is enciphered using the cryptographic key for personal identification numbers stored in IC card 31.
[0040] At step 8, to IC card 31, the READ command is published and the cryptographic key for a communication link and the decode key for a communication link which are stored in the elementary files 2, such as individual humanity news stored in the elementary file 1 of IC card 31, are read directly. In addition, the cryptographic key for a communication link and the decode key for a communication link cannot be read directly, but Card ID is required. Moreover, since it is enciphered, in order to read such key information, first, this card ID takes out a card ID decode key from the elementary file 1, and decrypts this card ID. And the cryptographic key for a communication link and the decode key for a communication link which are

stored in the elementary file 2 using this decrypted card ID are read. Thus, security nature is raised.
[0041] The read individual humanity news is stored in buffer memory 25 at step 9. At step 10, as shown in drawing 8 (C), the message "input the load amount of money" is displayed on a display 12, and the input of the load amount of money is demanded from an operator as dealings demand information. An operator inputs the predetermined load amount of money using a ten key 13 according to this message. At step 11, the inputted load amount of money is stored in buffer memory 25, and commo data is generated.
[0042] Drawing 9 is the explanatory view of operation showing the actuation in the first half of an example 1. As shown in this drawing 9 (A), Card ID, the account number, the load demand amount of money, a personal identification number, iris data, etc. are contained in this commo data, and data are added to a header and the back end at this head section.
[0043] At step 12, as shown in drawing 9 (B), data, such as the account number, the load demand amount of money, a personal identification number, and iris data, are enciphered among the commo data stored in buffer memory 25. In addition, a personal identification number is option data inputted in step 7, and it will be enciphered by the duplex when there is a personal identification number. Security nature is raised by this.

[0044] This encryption is performed using the cryptographic key for a communication link read in IC card 31. Although it is common to use DES (Data Encryption Standard) of a common key system, RSA of a public key system, etc. as a cipher system, it is not restricted to this method.
[0045] At step 13, it connects with a host computer 41 using the connection telephone number read in IC card 31, and this commo data is transmitted. However, the telephone number of a connection place host computer can also be inputted using a ten key 13.
[0046] Steps 14-16 are performed with a host computer 41. At step 14, as shown in drawing 9 (C), the received commo data is decrypted.
[0047] In order to decrypt commo data, the enciphered card ID is first picked out from commo data, and it decrypts using the decode key of the card ID in which this card ID is stored by the file 43. And a file 44 is searched by using the number of the decrypted card ID as a key, and the decode key for a communication link and the decode key for personal identification numbers are taken out from a file 44. Furthermore, commo data is decrypted using this decode key for a communication link. In addition, when the enciphered personal identification number is contained, this personal identification number is decrypted using the decode key for personal identification numbers.
[0048] Thus, since the decode key for a communication link and the decode key for personal identification numbers were taken out from the file 44 using the card ID transmitted from the coin box set 1, if this card ID is not known, these decode keys cannot be taken out, but security nature is guaranteed.
[0049] At step 15, a host computer 41 performs predetermined processing. Drawing 10 is the explanatory view of operation showing the actuation in the second half of an example 1. As shown in drawing 10 (A), the account number and the load demand amount of money are taken out from the decrypted commo data by processing of this host computer 41, and cybermoney is pulled out based on the account number. After processing termination, the account number, the load amount of money, and iris data are recorded on the file 42 for logs, and a transaction remains. the dealings candidate who certainly has an account by leaving a transaction -- proof of having loaded the amount of money to him remains.
[0050] At step 16, as shown in drawing 10 (B), the commo data with which Card ID, the account number, and the load amount of money were stored is formed, this account number and the load amount of money are enciphered using the cryptographic key for a communication link taken out from the file 44, and commo data as shown in drawing 10 (C) is generated. In addition, this cryptographic key for a communication link is taken out considering the number of the card ID which the above-mentioned decrypted as a key. The generated commo data is transmitted to the coin box set 1 of a transmitting agency, and a coin box set 1 performs steps 17-19.
[0051] At step 17, as shown in drawing 10 (D), commo data is received and it decrypts using the decode key for a communication link read in IC card 31. Consequently, commo data as shown in drawing 10 (E) is obtained. And the WRITE command is published and the load amount-of-money information stored in this commo data is stored in the load amount-of-money area of the elementary file of IC card 31.
[0052] At step 18, as shown in drawing 8 (D), while displaying the message, "thank you", a dealings date, the account number, the load amount of money, and a dealings serial number are displayed on the screen of a display 12. After a display, while making IC card 31 deactivate, IC card 31 is released from the IC card insertion opening 14.
[0053] At step 19, a result is printed in a receipt and this receipt is discharged from the receipt exhaust port

16. in addition, the step 5 -- him -- an authentication means -- steps 12 and 13 -- a terminal side transmitting means -- step 14 -- a host side receiving means -- step 16 is equivalent to a host side transmitting means, and step 17 is equivalent to a dealings processing means for step 15 at a terminal side receiving means.
[0054] <Effectiveness of an example 1> Since according to the example 1 a coin box set 1 is used as a terminal and it was made to perform loading of cybermoney using the telephone line 2 as explained above, if there is a coin box set 1 to which the general telephone line 2 was connected, it can communicate always anywhere, without using the circuit of dedication. For this reason, communication link cost can be reduced.
[0055] moreover, IC card 31 -- using -- off-line -- him -- the ** which does not cover a load over a host side since it attests and cybermoney was loaded -- him -- it can attest and, moreover, cybermoney can be loaded to insurance. moreover -- since cybermoney was loaded using iris data peculiar to him -- him -- by others of an except, the malfeasance of pulling out cybermoney can be prevented and a thoroughgoing system can be built on security.
[0056] Moreover, since this card ID was enciphered while having read the cryptographic key for a communication link, and the decode key in IC card 31, decrypting a communication link data encryption and the reply data from a host computer 41 using these two keys and reading two keys further using this card ID, even when the general telephone line 2 is used, it can communicate safely.
[0057] Moreover, since it prevented from taking out the cryptographic key for a communication link etc. simply by the third person who does not know this card ID as this enciphered card ID was transmitted to a host computer 41, this card ID was decrypted and the cryptographic key for a communication link etc. was taken out from a file 44 using this card ID, security nature improves.
[0058] Moreover, since it was made to connect with a host computer 41 automatically using the connection telephone number read in IC card 31 when transmitting commo data to a host computer 41 from a coin box set 1, an operator's burden can be reduced.
[0059] Furthermore, in a host computer 41 side, since an operator's iris data are registered and it left the transaction when processing pulled down from an account was performed, he can leave proof of having loaded cybermoney, and when a crime etc. occurs, it should use for the solution.
[0060] in addition, by this example 1, in step 7, although the personal identification number was inputted as an option, a personal identification number is inputted -- making -- iris data and a personal identification number -- using together -- him -- it may be made to attest. Moreover, although it was made to encipher to a duplex about this personal identification number, if security nature is guaranteed, encryption by the cryptographic key for personal identification numbers is also omissible.
[0061] <Example 2> Using a personal computer as a terminal, an example 2 connects the telephone line to this personal computer, and is made to perform loading of cybermoney from a personal computer.
[0062] Drawing 11 is the block diagram showing the configuration of an example 2, and drawing 12 is the explanatory view showing the appearance of the system equipped with the configuration of drawing 11 . As shown in drawing 12 , a personal computer 51 is a personal computer of the note type which was equipped with the display 52 of a liquid crystal display, and the keyboard 53, and equipped the upper part of a display 52 with the camera 54 further.
[0063] IC card reader writer 56 for writing the mouse 55 for inputting predetermined data and the data to IC card 31 and the telephone line 2 are connected to this personal computer 51.
[0064] As shown in drawing 11 , the display 52, the mouse 55, and the keyboard 53 are connected to the control section 21. By the example 2, SAM24 is built in IC card reader writer 56. In addition, the same sign is attached about the same element as an example 1, and explanation is omitted.
[0065] <Actuation> When performing loading of cybermoney using a personal computer 51, IC card 31 is inserted in IC card reader writer 56. Mutual recognition is performed after insertion between IC card 31 and SAM24 built in IC card reader writer 56. And loading of cybermoney is performed like an example 1.
[0066] <Effectiveness of an example 2> Since it was made to perform loading of cybermoney using the flexible personal computer 51 according to the example 2 as explained above, if there is the telephone line 2, cybermoney can be loaded always anywhere easily also at a home also in office.
[0067] In addition, although this example 2 explained the case where the personal computer of a note type was used, it is not restricted to this and the personal computer of a stand-alone mold can also be used.

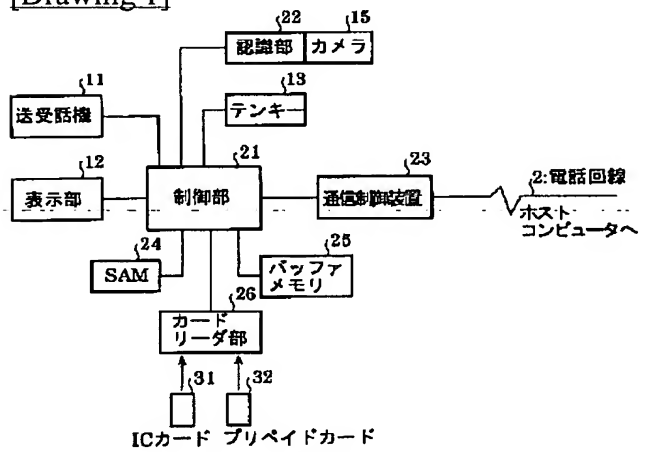
[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

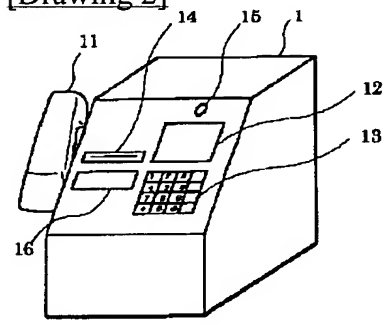
DRAWINGS

[Drawing 1]



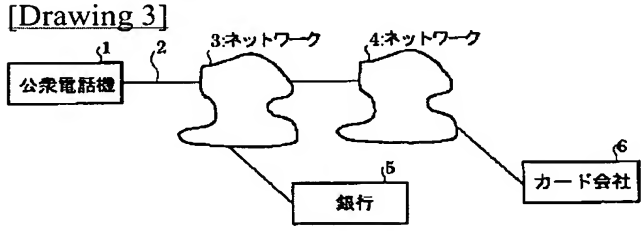
具体例１の構成を示すブロック図

[Drawing 2]



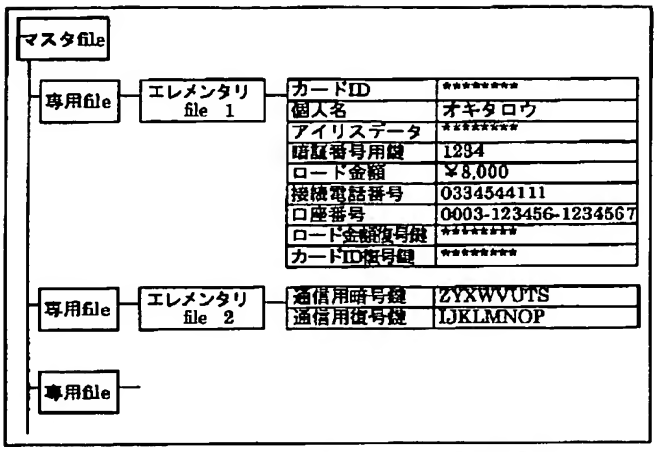
具体例１の公衆電話機の外観を示す斜視図

[Drawing 3]



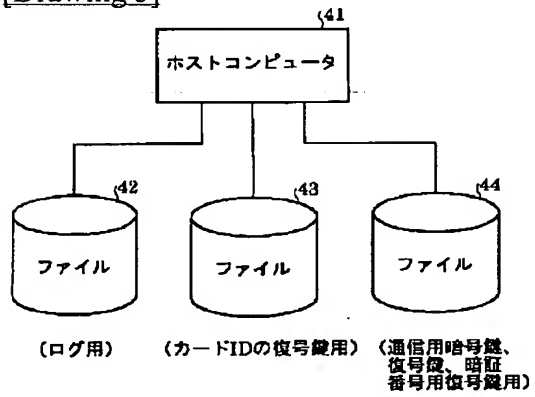
具体例１のシステム構成図

[Drawing 4]



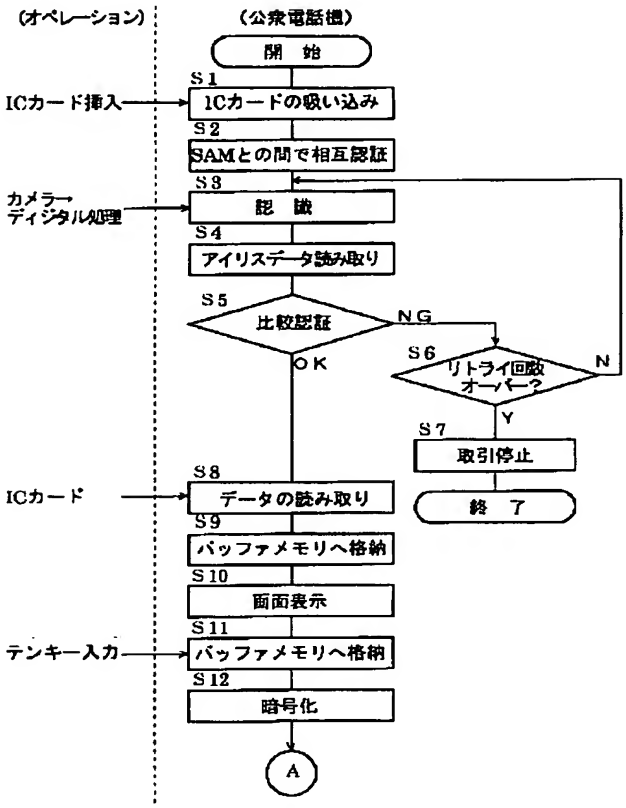
具体例１のICカードのファイル構成を示す説明図

[Drawing 5]



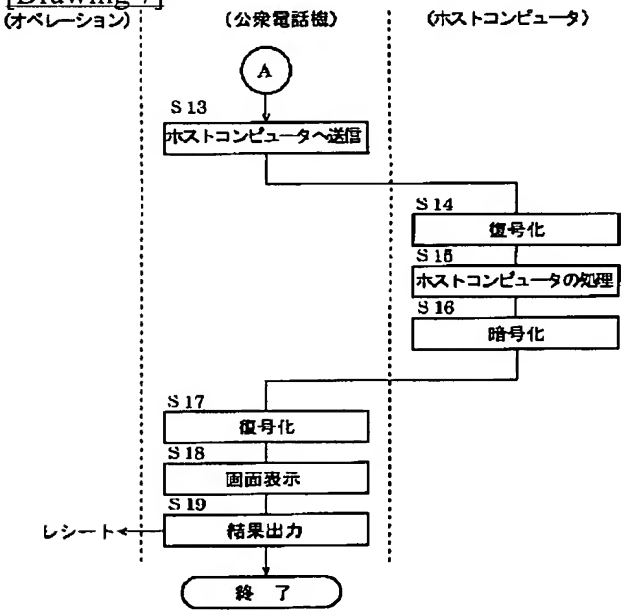
具体例１のホストコンピュータの構成を示すブロック図

[Drawing 6]



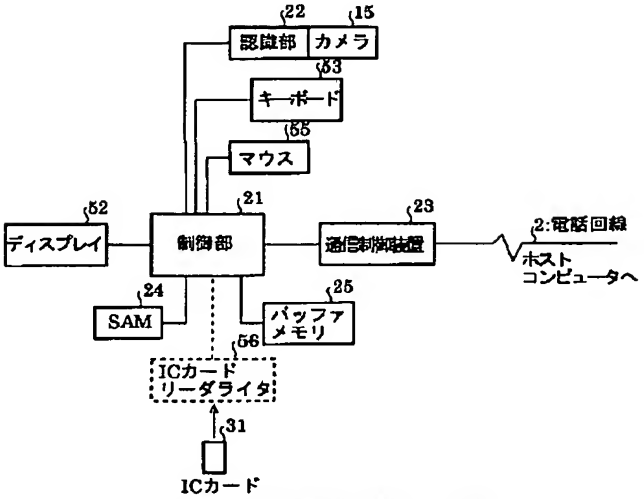
具体例１の動作を示すフローチャート（その１）

[Drawing 7]



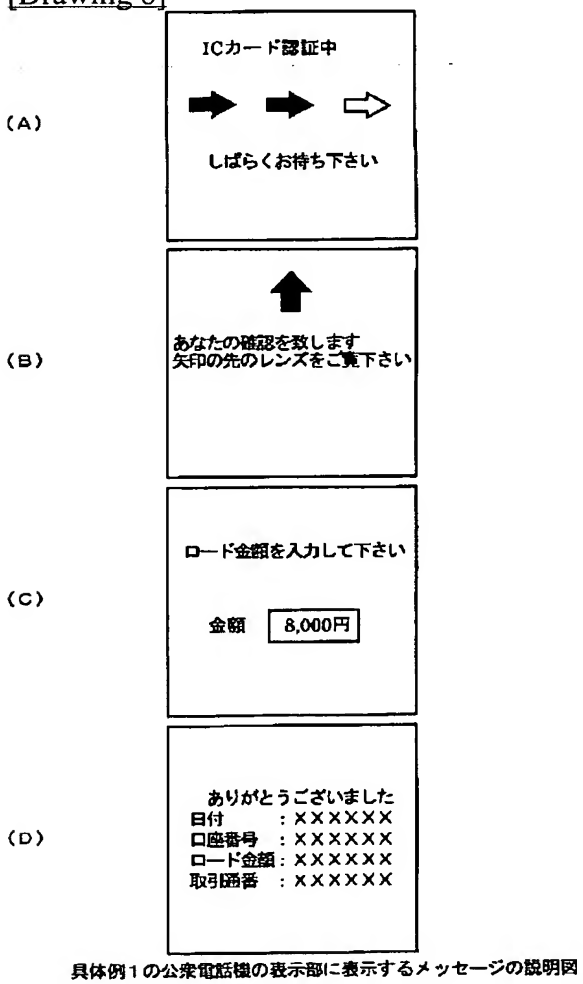
具体例１の動作を示すフローチャート（その２）

[Drawing 11]



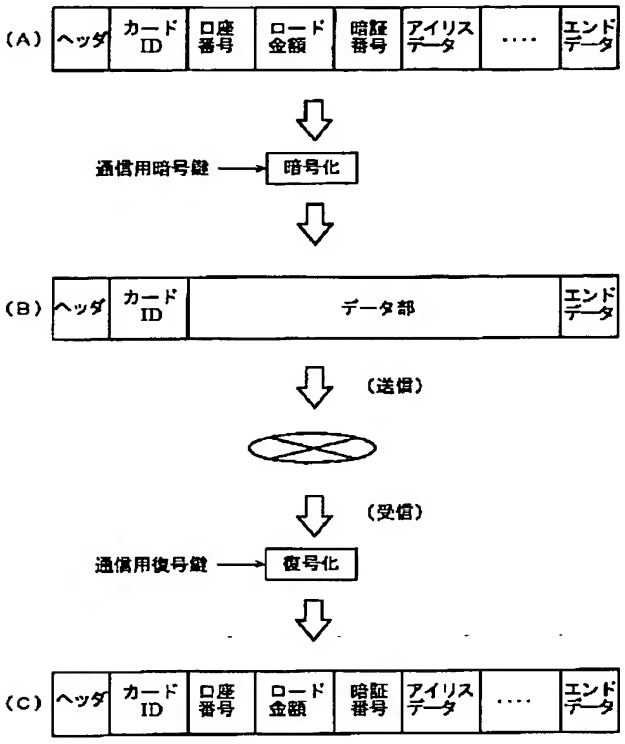
具体例２の構成を示すブロック図

[Drawing 8]



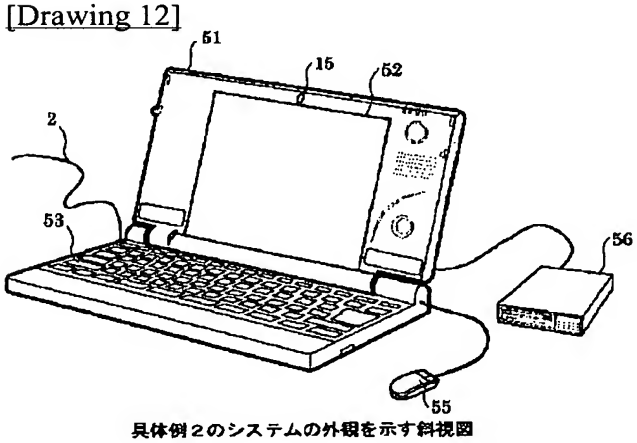
具体例１の公衆電話機の表示部に表示するメッセージの説明図

[Drawing 9]



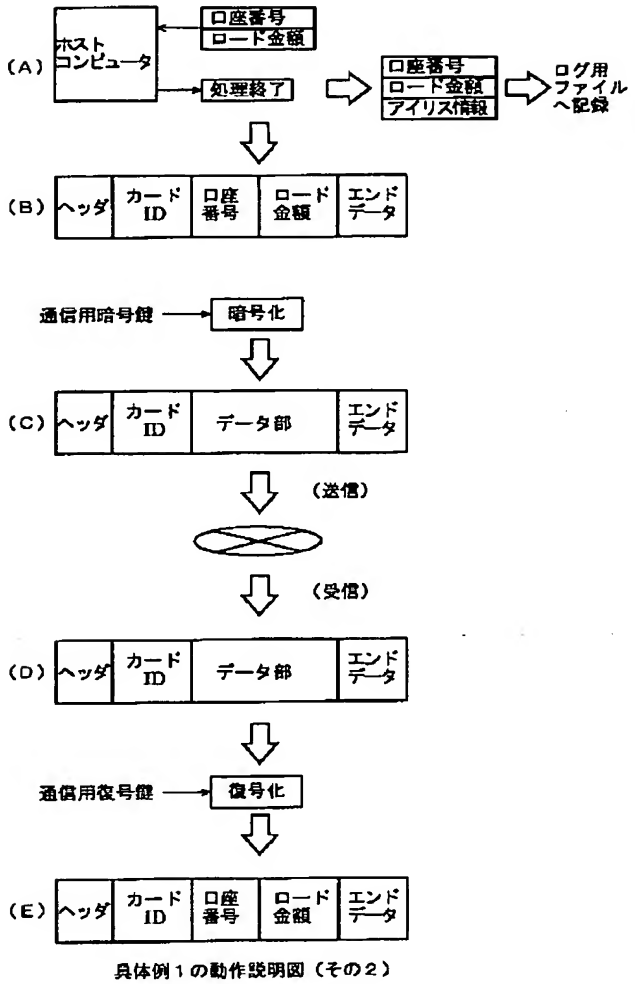
具体例１の動作説明図（その１）

[Drawing 12]



具体例２のシステムの外観を示す斜視図

[Drawing 10]



具体例１の動作説明図（その２）

[Translation done.]